BLIND EXCHANGE OF KEYS USING AN OPEN PROTOCOL

ABSTRACT

A computer system and method where a user is authenticated to both an authentication server and to a client machine, but no link between the client machine and authentication server is needed. Login information is provided from the client machine to the technician machine in an encrypted format using a public key so that the technician machine cannot access the login information. The technician machine communicates the encrypted login information to an authentication server, which decrypts the login information using a private key and provides the decrypted login information to the technician machine if the technician machine can authenticate itself to the authentication server. The invention is particularly useful in enabling field service technicians to access client computer systems from remote locations such as field offices, hotel rooms, airports and the like.